(19) Canadian Intellectual Property Office
An Agency of Industry Canada

Office de la Propri,t, Intellectuelle du Canada
Un organisme d'Industrie Canada

(11) CA 2 308 697 (13) A1

(40) 15.11.2001
(43) 15.11.2001

(12)

(21) 2 308 697

(51) Int. Cl.7: H04L 12/56, H04L 12/24

(22) 15.05.2000

(71) NORTEL NETWORKS LIMITED,
World Trade Center of Montreal
380 St. Antoine Street West
8th Floor, MONTREAL, Q1 (CA).

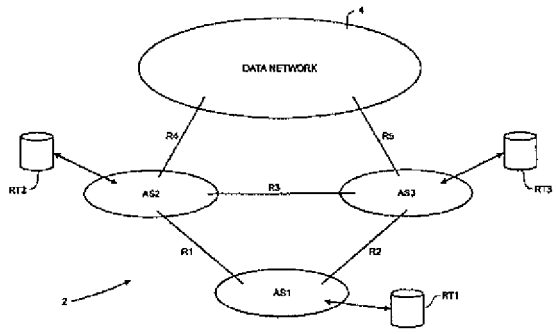
(72) JAMIESON, DWIGHT D. (CA).
MAALOUF, RABIH (CA).
ZHOU, WEI (CA).

(74) SWABEY OGILVY RENAULT

(54) ROUTES D'EXCLUSION DANS DES ROUTEURS AVEC PROTOCOLE DE PASSERELLE FRONTIERE (BGP)
(54) EXCLUSION ROUTES IN BORDER GATEWAY PROTOCOL (BGP) ROUTERS

(57)

2222 Efficient control of packet forwarding by a router²is enabled by storing in a forwarding table information²explicitly identifying exclusion routes to which packets²may not be forwarded. An exclusion route includes the same²attributes as a conventional "inclusionary" route, and thus²will be returned from a forwarding table for any matching²packets using conventional best-match algorithms. The²exclusion route is identified by a zero fill of its Next² Hop attribute, which indicates that the exclusion route is²inaccessible. Any packets matching an exclusion route are²discarded. This permits access control to selected²addresses in the network space.22



Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2308697 A1 2001/11/15

(21) 2 308 697

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(22) Date de dépôt/Filing Date: 2000/05/15

(41) Mise à la disp. pub./Open to Public Insp.: 2001/11/15

(51) Cl.Int.^{7}/Int.Cl.^{7} H04L 12/56, H04L 12/24

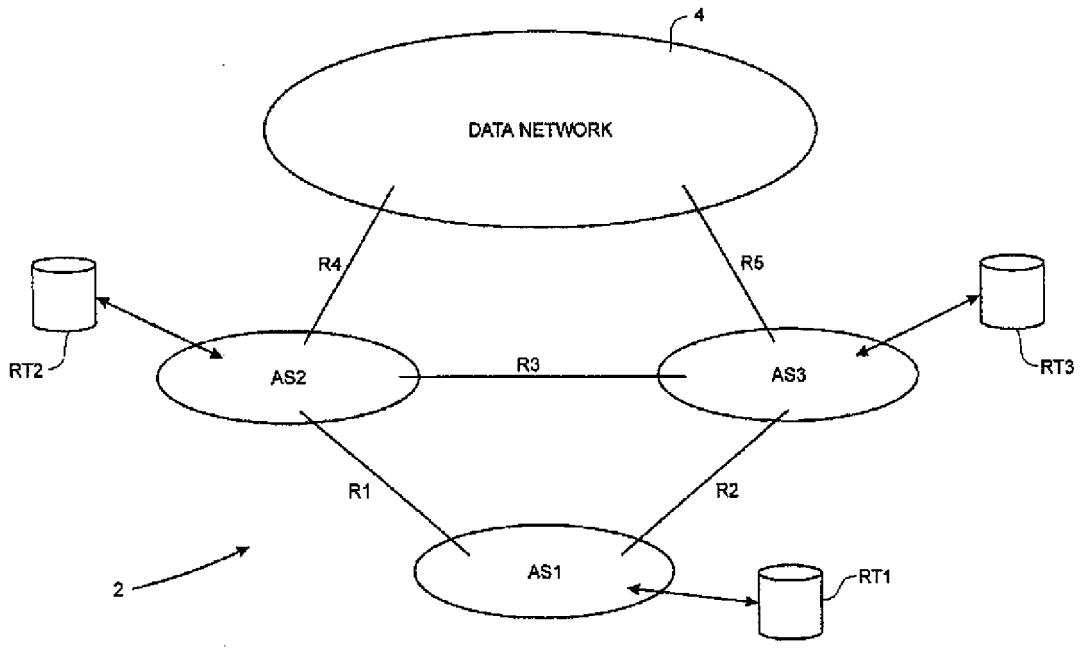
(71) Demandeur/Applicant:
NORTEL NETWORKS LIMITED, CA

(72) Inventeurs/Inventors:
JAMIESON, DWIGHT D., CA;
ZHOU, WEI, CA;
MAALOUF, RABIH, CA

(74) Agent: SWABEY OGILVY RENAULT

(54) Titre : ROUTES D'EXCLUSION DANS DES ROUTEURS AVEC PROTOCOLE DE PASSERELLE FRONTIERE (BGP)

(54) Title: EXCLUSION ROUTES IN BORDER GATEWAY PROTOCOL (BGP) ROUTERS



(57) Abrégé/Abstract:
Efficient control of packet forwarding by a router is enabled by storing in a forwarding table information explicitly identifying exclusion routes to which packets may not be forwarded. An exclusion route includes the same attributes as a conventional "inclusionary" route, and thus will be returned from a forwarding table for any matching packets using conventional best-match algorithms. The exclusion route is identified by a zero fill of its Next Hop attribute, which indicates that the exclusion route is inaccessible. Any packets matching an exclusion route are discarded. This permits access control to selected addresses in the network space.

ABSTRACT OF THE DISCLOSURE

Efficient control of packet forwarding by a router is enabled by storing in a forwarding table information explicitly identifying exclusion routes to which packets may not be forwarded. An exclusion route includes the same attributes as a conventional "inclusionary" route, and thus will be returned from a forwarding table for any matching packets using conventional best-match algorithms. The exclusion route is identified by a zero fill of its Next Hop attribute, which indicates that the exclusion route is inaccessible. Any packets matching an exclusion route are discarded. This permits access control to selected addresses in the network space.

EXCLUSION ROUTES IN BORDER GATEWAY PROTOCOL (BGP) ROUTERS

CROSS-REFERENCE TO RELATED APPLICATIONS

This is the first application filed for the present invention.

MICROFICHE APPENDIX

Not Applicable.

TECHNICAL FIELD

The present invention relates to routing protocols for connectionless traffic in a data network, and in particular to explicitly defined exclusion routes in border gateway protocol (BGP) routers of a data network.

BACKGROUND OF THE INVENTION

The modern data network space is made up of a plurality of autonomous systems that are directly or indirectly linked to a data network, such as the internet. In this respect, it will be noted that the classical definition of an "autonomous system" refers to a set of one or more routers under a single technical administration, using an interior gateway protocol (IGP) and common metrics to route packets within the autonomous system, and using an exterior gateway protocol (EGP) to route packets to other autonomous systems. Since this classic definition was developed, it has become common for single autonomous systems to use several interior gateway protocols and sometimes several different sets of metrics within an AS.

In the present application, the term autonomous system is used to emphasize the fact that, even when multiple IGPs and metrics are used, the technical administration of an AS appears to other autonomous systems to have a single coherent interior routing plan and presents a consistent picture of what destinations are reachable through it.

Fig. 1 is a block diagram showing three autonomous systems (AS1, AS2 and AS3) that are linked together and to a data network (e.g. the internet) by means of links R1 through R5. The relationship between autonomous systems illustrated in Fig. 1 is typical of that set up to connect an enterprise domain (such as a corporate local area network) represented at AS1 to the internet via a pair of internet service providers respectively represented at AS2 and AS3. Interaction between each of the autonomous systems (that is, over links R1 through R5), including transfer of route information is controlled by BGP. BGP may also be used to control routing within the data network. Within each of the autonomous systems, an interior gateway protocol is used to control the routing of traffic. Any of a variety of interior gateway protocol implementations may be used for this purpose. Exemplary interior gateway protocol implementations include the routing information protocol (RIP) and the Open Shortest Path First (OSPF) protocol. Using this arrangement, information concerning addresses that are reachable through the internet can be obtained by the autonomous systems AS2 and AS3 using BGP update messages received over links R3 and R4 respectively. The autonomous system AS1 is then able to obtain information concerning routes that are reachable through

AS2 by means of BGP update messages received over link R1. Similarly, AS1 is able to obtain information concerning routes that are reachable through AS3 by means of BGP update messages received over link R2.

In the modern data network space, packetized data traffic is transported using an assortment of different protocols (e.g. multi-protocol label switching [MPLS]; internet protocol [IP], frame relay, asynchronous transfer mode [ATM], etc.). Some of these protocols, such as ATM, are connection-oriented, in packets are propagated across the network space hop-by-hop along a path that is set up at the beginning of a communications session. Other protocols, (such as IP) which do not transport data over predefined end-to-end paths are referred to as "connectionless".

Connectionless traffic is normally routed across a communications network using a shortest-path or least-cost-path routing protocol. Typical examples of such routing protocols include the Interior Gateway Protocol (IGP), and the Exterior Gateway Protocol (EGP). IGP is designed to handle routing of traffic within an autonomous system, while EGP is used for routing traffic between autonomous systems. The Border Gateway Protocol (BGP) is an evolution of the EGP. A recently released version of BGP (BGP-4) is capable of routing traffic both within and between autonomous systems.

Each of these routing protocols operates on the basis of a forwarding or routing table, which is maintained by a routing table manager (RTM) and used to map

received packets to downstream links. The forwarding table contains information identifying routes to which packets can be forwarded. Exemplary data fields within the forwarding table include: IP Address; Mask; Route; Next Hop and Next Hop Interface. As each packet arrives at a router, its destination address is read and used to query the forwarding table. If a matching route in the forwarding table is located, the corresponding Next Hop and Next Hop Interface fields are used to forward the packet to a downstream link towards its destination. Otherwise, the packet is discarded.

The routes identified in the forwarding table are always "inclusionary", in the sense that a router can forward packets to any route identified in the forwarding table. Conversely, the router is unable to forward packets to any routes that are not identified in the forwarding table. Typically, the forwarding table contains a list of explicitly defined routes to which packets may be forwarded, and/or a default route to which the router forwards packets that do not match any of the explicitly defined routes.

The use of a comprehensive list of accessible (explicitly defined) routes enables maximum routing flexibility, and thus is generally favored for routers within the network core, as well as for access servers (e.g. maintained by network service providers) where routing flexibility is very desirable. This method also provides a high level of control over forwarding of traffic to any particular route or destination on the network. For example, if it is desired to restrict or prohibit

forwarding of traffic to any particular route or destination address, then the associated route is simply removed from the forwarding table. However, a limitation of this method is the size of the forwarding table. At present, the internet comprises in excess of 70,000 routes, all of which must be registered in the forwarding table to permit the router to forward packets to destination addresses subtending those routes. This large number of routes, which is rapidly increasing, imposes a heavy demand on router resources. This leads to a requirement for more powerful (and thus expensive) router equipment to achieve satisfactory performance.

The use of a forwarding table containing a single default route sacrifices routing flexibility to obtain maximum throughput performance with minimum system resources. Consequently, this method has found favor for use in domain servers, such as gateway routers serving autonomous systems and corporate networks. Such systems are commonly connected to the internet through an access server through which all traffic is directed. In this case, the default route of the forwarding table identifies the access server, and thus all traffic originating in the domain is routed to the access server irrespective of the destination address of any particular packet. In practice, this does not impose any real limitations on routing flexibility, since all traffic originating on the domain passes through the access server in any event. However, this technique dramatically reduces the size of the forwarding table, thereby permitting the use of smaller

(and therefore less expensive) routers, without sacrificing performance.

A limitation of this method is that since all traffic is forwarded to the access server, the routing protocol of the domain server cannot be used to restrict or prohibit forwarding packets to any particular routes or destinations. As a result, policies restricting the forwarding of packets are typically implemented by route and/or packet filtering algorithms, which may be provided as part of a firewall or router application. However, these solutions increase the complexity of forwarding applications, and often contribute to scalability issues because system performance often degrades rapidly as the number of restricted routes increases.

Accordingly, a system for enabling policy-based restriction of packet forwarding to one or more routes, that can be implemented at the level of the routing protocol, while minimizing system resource requirements, remains highly desirable.

SUMMARY OF THE INVENTION

An object of the invention is to provide a method of enabling efficient policy-based restrictions on packet forwarding by a routing protocol.

A further object of the present invention is to provide an extension to Border Gateway Protocol (BGP) to enable efficient policy-based restrictions on packet forwarding.

Accordingly, an aspect of the present invention provides a method of enabling efficient restrictions on packet forwarding by a router having a forwarding table. The method comprises steps of: storing in the forwarding table information explicitly identifying an exclusion route to which packets may not be forwarded; and discarding any packet having a respective destination address matching the exclusion route.

Another aspect of the present invention provides a router for forwarding connectionless packet traffic through a network space, the router comprising a forwarding table adapted to store information explicitly identifying exclusion routes to which packets may not be forwarded.

Each exclusion route is preferably identified by a respective predetermined value of a selected field of the forwarding table. The selected field may be a "Next Hop" field, and the predetermined value can be a zero fill of the Next Hop field (e.g. "0.0.0.0").

Information explicitly identifying any included routes to which packets may be forwarded can also be stored in the forwarding table. In some embodiments, information identifying a single included route is stored in the forwarding table as a default route to which all packets having a destination address that does not match an exclusion route are forwarded.

An advantage of the present invention is that the forwarding of frames can be controlled on a route-by-route basis with minimum demand on system resources within the router.

BRIEF DESCRIPTION OF THE DRAWINGS

Further features and advantages of the present invention will become apparent from the following detailed description, taken in combination with the appended drawings, in which:

Fig. 1 is a block diagram schematically illustrating a data network in which the present invention may be utilized; and

Fig. 2 shows a schematic representation of a portion of a forwarding table in accordance with an embodiment of the present invention.

It will be noted that throughout the appended drawings, like features are identified by like reference numerals.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention provides a system for controlling the forwarding of connectionless traffic across a communications network. As shown in Fig. 1, a communications network 2 in which the present invention may be utilized generally comprises a plurality of autonomous systems (ASs) connected to a data network 4, such as, for example, the internet. In the exemplary embodiment of Fig. 1, three autonomous systems (AS1, AS2 and AS3) are shown, interconnected by links R1, R2 and R3. AS2 and AS3 are further connected to the data network 4 through links R4 and R5 respectively. This arrangement is typical of connection schemes for providing internet access to an enterprise, for example. Thus, AS1 may be implemented as a

corporate local area network (LAN), which is connected to the data network 4 (e.g. the internet) using a pair of service providers (ISPs) at AS2 and AS3 respectively.

Each autonomous system comprises one or more routers (not shown), under a single technical administration, and transport of data packets within an autonomous system is controlled using one or more implementations of the Interior Gateway Protocol (IGP). As is known in the art, a router may be implemented as physical hardware or as a virtual router running in a server, for example. Exemplary implementations of IGP used for the transport of packet data traffic within an autonomous system include: routing information protocol (RIP); and Open Shortest Path First (OSPF). Transport of packet data traffic over links R1 - R5, that is, between AS1, AS3 and AS3, and between AS2 and AS3 and the data network 4, is controlled by an implementation of the border gateway protocol (BGP).

As is well known in the art, forwarding of traffic under the BGP is controlled by a forwarding or routing table (RT) which is maintained by a routing table manager (RTM - not shown) and accessible to each router. Thus each autonomous system AS1 - AS3 is provided with at least one respective routing table RT1-RT3 A routing table will normally be co-resident with a respective router, but may be maintained at a remote location and accessible through the network. Under the BGP, each route that is reachable through a router is explicitly identified in the respective routing table. Exemplary data fields used to identify

routes in the forwarding table include: Mask 6; Route 8; Next Hop 10; and Next Hop Interface 12 (see Fig. 2).

As mentioned previously, each autonomous system AS1 - AS3 may comprise one or more routers (which may be implemented as virtual routers), and each router will normally have a respective routing table. However, for simplicity of description, in the illustrated embodiment, AS1 is assumed to include a single router, which handles all traffic flow through links R1 and R2 between AS1 and AS2 and AS3 using a respective routing table RT1. AS2 and AS3 are assumed to each include a respective single router, which handle all traffic flow between AS1 and other points in the communications network 2 using respective routing tables RT2 and RT3. Both of these routing tables (RT2 and RT3) will generally contain a comprehensive listing of every route that is reachable by AS1 through the respective autonomous system. This affords maximum routing flexibility for forwarding connectionless traffic through the communications network 2. Additionally, AS2 and AS3 may adjust the content of their respective routing tables RT2 and RT3 on the basis of policies that are specific to AS1.

As shown in Fig. 2, in order to minimize demand on system resources, AS1 (Fig. 1) is provisioned with a respective routing table RT1 containing a default route 18. As shown in Fig. 2, the default route 14 is identified by a zero fill (i.e. "0.0.0.0") of the Route field 8 in the routing table RT1. The forwarding address stored in the Next Hop field 10 identifies a selected one of AS2 and AS3. In the absence of a route matching the destination address

of a packet, conventional best-match searching algorithms will return the default route 18.

For the purposes of the present example, it will be assumed that the Next Hop field 10 of the default route 14 identifies AS2. As a result, every packet originating on AS1 and destined for an address outside of AS1 will be automatically forwarded to AS2, unless the routing table RT1 contains other routes which match the packet destination address. AS2 then uses its own forwarding table RT2 to forward those packets towards their destinations.

It will be noted that in Fig. 2, no values are shown for the Next Hop Interface field 12 of the routing table RT1. It will be appreciated that this field will normally contain non-zero values that, in general, will depend on the specifics of each route, and are not material to the present invention. Accordingly, they are omitted from the illustration of Fig. 2.

In accordance with the present invention, improved control over routing of traffic originating in AS1 is enabled by storing one or more "exclusion routes" 16 (one is illustrated in Fig. 2) in the routing table RT1, in addition to the default route 18. The exclusion route 20 differs from conventional inclusionary routes (including the default route 14) in that it explicitly identifies a route to which traffic may not be forwarded. The exclusion route 16 preferably possesses the same number and type of attributes as a conventional (inclusionary) route. As a result, no modifications are required in the routing table or routing table manager to accommodate the insertion of

one or more exclusion routes 16. Additionally these routes will match packets destined to them using conventional best-match algorithms, so that the exclusion route 16, rather than the default route 14 will be automatically returned for matching packets. The primary differences between an exclusion route 16 and conventional (inclusionary) routes lay in the value of the Next Hop attribute 10, and the way in which that value is interpreted by the packet forwarding algorithm of the autonomous system AS1.

In particular, as shown in Fig. 2, the exclusion route 16 has a Next Hop 10 value that is zero-filled (i.e. "0.0.0.0"). It will be seen that this differs from the default route 14, in which the Route attribute is zero-filled (i.e. "0.0.0.0") and the Next Hop attribute contains a forwarding address (e.g. identifying AS2). A zero fill of the Next Hop attribute 10 is interpreted by the packet forwarding algorithm running of AS1 as a non-reachable route, and any packets having a destination address matching the exclusion route 16 are discarded.

Various methods may be used to create exclusion routes. Exemplary methods include: local creation of exclusion routes based on import policies; and remote creation of exclusion routes. Each of these methods are described in greater detail below, first in general terms, and then by way of specific example with reference to Figs. 1 and 2.

Exclusion routes can be created locally based on BGP import policies. As is known in the art, standard BGP

provides a mechanism by which a router can create and remove routes (that is, store route information in and delete route information from its routing table) in response to update messages received from another router. The response of the router to each update message can be controlled by means of import policies defined for the router. In general, an import policy defines the actions that are to be taken in the event that an update message matches a set of predetermined criteria. These criteria normally include predetermined values of any route attribute, which may be well known attributes or a private attribute assigned by a peer router in accordance with a service agreement, for example.

Conventionally, BGP import policies provide two alternative actions that can be taken when an update message contains route information matching the defined criteria: either the update message is ignored, or a new (inclusionary) route is created so that packets may be forwarded to that route. In accordance with the present invention, this facility can be extended to also enable the creation of exclusion routes. This provides a convenient, policy-based method for creating exclusion routes based on received update messages.

In accordance with the present invention, exclusion routes can also be remotely created. In one embodiment, this may be accomplished by defining an "exclusion" message type. Thus, a first router can send an exclusion-type update message to a peer router, identifying itself (the first router) in the Route attribute. This exclusion-type update message, including the self-identifying Route

attribute, can then be used by the peer router, in accordance with its own import policies, to create an exclusion route identifying the first router. As a result of this action, the packet forwarding algorithm in the peer router will recognize the route to the first router as an exclusion route, and any packets arriving at the peer router and destined for the first router will therefore be discarded.

In the following discussion, a number of examples of the use of exclusion routes are provided.

Example 1: Exclusion Routes Used to Restrict Access to Selected Routes;

Exclusion routes can readily be created by AS1 to restrict (or prevent) access to certain predetermined routes or destination addresses through the communications network. In a simple embodiment, this can be accomplished by defining an import policy for AS1 that matches on an attribute identifying the restricted route (e.g. the IP Address attribute) Subsequently, any update messages received by AS1 and matching the selected criteria, will result in the creation of an exclusion route 16 in the routing table RT1. As a result of this action, packets originating in AS1 and destined for the restricted route (e.g. to request a download of data) will be discarded by AS1, so that access to the restricted route by users of AS1 is prevented.

A more complex embodiment involves the assignment of a private attribute value to a selected set of routes by a service provider, and then using the assigned attribute as the basis for creating exclusion routes. For example,

AS1 may wish to prevent access to certain target addresses (e.g. addresses carrying pornographic content). Thus AS1 and a service provider at AS2 may enter into an agreement according to which AS2 will attach a predetermined private attribute (such as a community tag) to any update messages propagated from any of the target addresses. AS1 can then define an import policy so that any update messages received from AS2 and bearing the predetermined local attribute will result in the creation of an exclusion route 16 in the routing table RT1. As a result of this action, packets originating in AS1 and destined for any of the target addresses (e.g. to request a download of data) will be discarded by AS1, so that access to the target addresses by users of AS1 is prevented.

Example 2: Traffic engineering

This example illustrates the use of exclusion routes for traffic engineering. In particular, AS1 may wish to use AS2 (via link R1) for outgoing traffic only, and AS3 (via link R2) for incoming traffic only. In this case, AS1 can create a conventional default route 14 in routing table RT1 which identifies AS2 in the Next Hop attribute 10. Thus any packets originating on AS1 and destined for routes outside to AS1 will be forwarded through link R1 to AS2 in an conventional manner.

AS1 can then use remote creation of an exclusion route to control incoming traffic. In particular, AS1 can formulate and send an exclusion-type update message to AS2 identifying itself (AS1) in the Route attribute. This update message can then be used by AS2 to create an exclusion route 16 in its routing table RT2 identifying

AS1. As a result, any packets arriving at AS2 and destined for AS1 will be discarded, and consequently AS1 will only receive packets from AS3, which is the desired result.

This operation may be enhanced by identifying link R1 in the Next Hop Interface 12 attribute of the update message sent by AS1 to AS2. Consequently, the routing table RT2 can identify "AS1 through link R1" as the exclusion route 16. The packet forwarding algorithm running in AS2 may then recognize that AS1 is reachable through AS3, and thus forward packets arriving at AS2 and destined for AS1, through link R3 to AS3. Again, the desired result is obtained, in that AS1 will only receive packets from AS3.

Example 3: Subscriber-specific service offering

As mentioned above, a service provider (e.g. at AS2 or AS3) can implement one virtual router and an associated routing table for each subscriber connection. This allows the service provider to implement exclusion routes on behalf of the subscriber.

As discussed in Example 1 above, a service provider can assign private attributes (such as a community tag) to a selected set of routes. This concept can be extended to enable a service provider to define a number of categories (e.g. based on content or some other attribute) and assign a respective community tag to the members of each category. A subscriber, would then be able to select (e.g. using an account management window accessed by the subscriber after logging into the service provider's server) any categories that they do not wish to access. This selection can then

be used to define an import policy for a subscriber-specific virtual router (instantiated when the subscriber logs onto the system) such that any routes matching the selected categories are identified in the routing table as exclusion routes. As a result, packets originating from the subscriber and destined for any route matching one of the selected categories will be discarded to thereby preclude access to those routes by the subscriber.

Because the subscriber's selection of restricted sites is implemented on a subscriber-specific virtual router that is instantiated when the subscriber logs into the service provider's server, system resources required to implement this function are minimized, and other subscribers are not affected. Furthermore, this functionality can be provided by the service provider even in cases where the subscriber is not capable of using BGP.

Thus it will be seen that the present invention provides an efficient technique for controlling the forwarding of connectionless traffic by a router.

The embodiments of the invention described above are intended to be exemplary only. The scope of the invention is therefore intended to be limited solely by the scope of the appended claims.

WE CLAIM:

1. A method of enabling efficient restriction of packet forwarding by a router having a forwarding table, the method comprising the steps of:

   a) storing in the forwarding table information explicitly identifying an exclusion route to which packets may not be forwarded; and

   b) discarding any packet having a respective destination address corresponding to any exclusion route identified in the forwarding table.

2. A method as claimed in claim 1, wherein each exclusion route is identified by a respective predetermined value of a selected field of the forwarding table

3. A method as claimed in claim 2, wherein the selected field is a "Next Hop" field.

4. A method as claimed in claim 3, wherein the predetermined value is a zero fill in each portion of the Next Hop field.

5. A method as claimed in claim 1, further comprising a step of storing in the forwarding table information explicitly identifying an inclusionary route to which packets may be forwarded.

6. A method as claimed in claim 5, wherein information identifying a single inclusionary route is stored as a default route in the forwarding table.

7. A method as claimed in claim 1, wherein the step of storing information explicitly identifying an exclusion route is performed in response to reception of an update message containing information identifying the exclusion route.

8. A method as claimed in claim 1, wherein the step of storing information explicitly identifying an exclusion route is performed in accordance with an import policy.

9. A method as claimed in claim 8, wherein the step of storing information explicitly identifying an exclusion route is performed in response to reception of an update message containing information identifying either one of an inclusionary route and an exclusion route.

10. A router for forwarding connectionless packet traffic through a network space, the router comprising a forwarding table adapted to store information explicitly identifying exclusion routes to which packets may not be forwarded.

11. A router as claimed in claim 10, wherein each exclusion route is identified by a respective predetermined value of a selected field of the forwarding table.

12. A router as claimed in claim 11, wherein the selected field is a "Next Hop" field.

13. A router as claimed in claim 12, wherein the predetermined value is a zero fill of the Next Hop field.

14. A router as claimed in claim 10, further comprising means for discarding any packet having a destination address corresponding to an exclusion route.

SWABEY OGILVY RENAULT

Suite 1600
1981 McGill College Avenue
Montreal, Quebec, Canada
H3A 2Y3

Patent Agents for the Applicant.

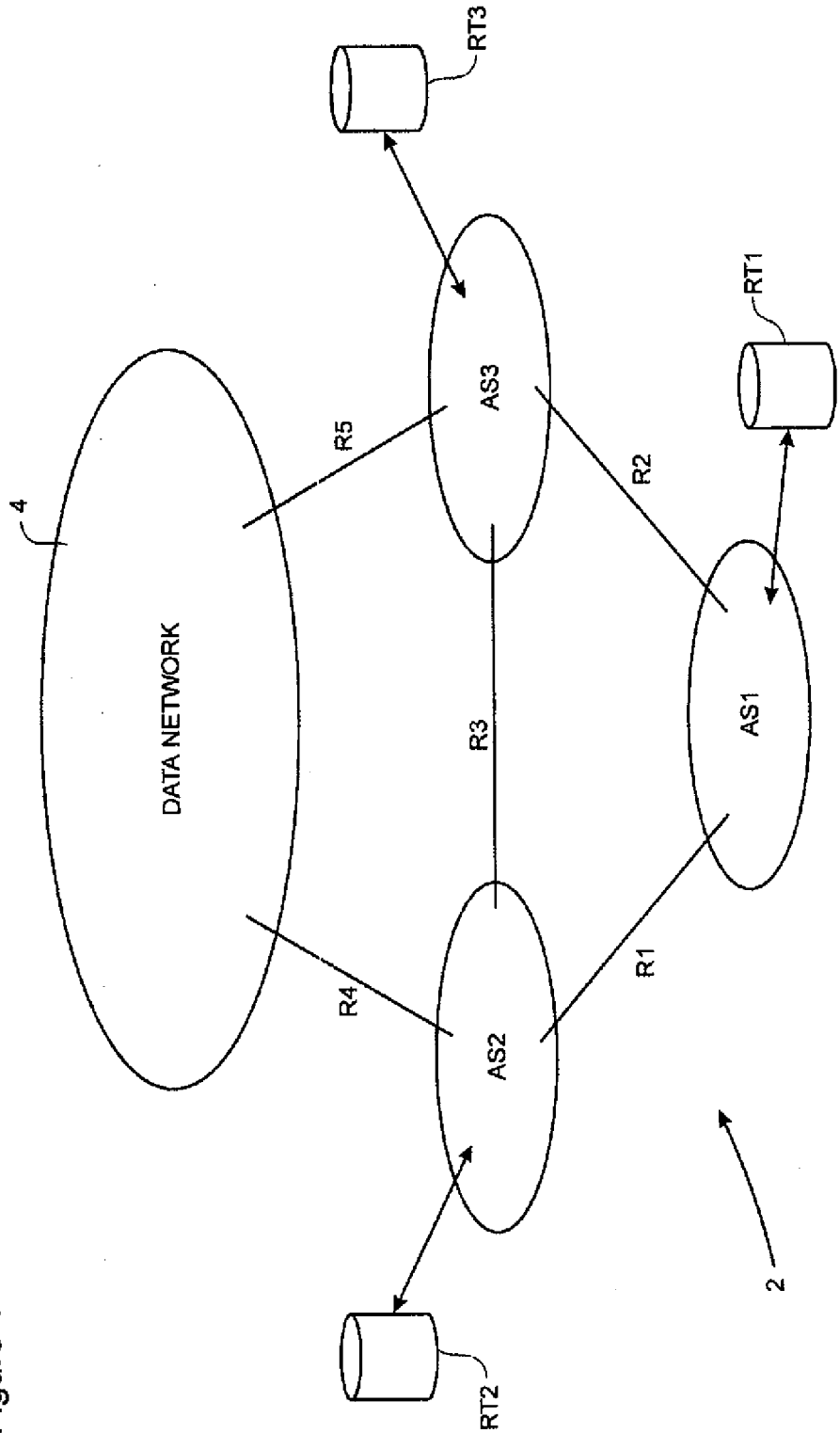


Figure 1

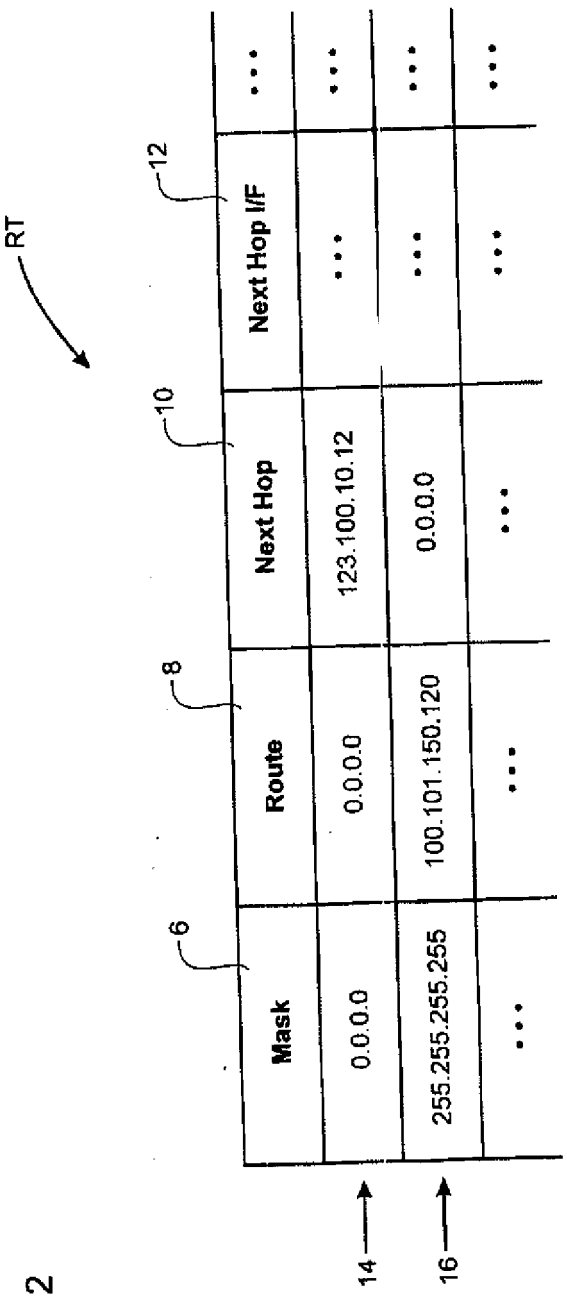

RT
6
8
10
12
Mask
Route
Next Hop
Next Hop I/F
0.0.0.0
0.0.0.0
123.100.10.12
255.255.255.255
100.101.150.120
0.0.0.0
14
16

Figure 2